Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DEPARTEMENTAAL VERTROUWELIJK

Logius

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.logius.nl
[redacted]@logius.nl

Inlichtingen bij

Datum
25 november 2020

memo

Bijdrage van Logius aan Veilig Met Corona

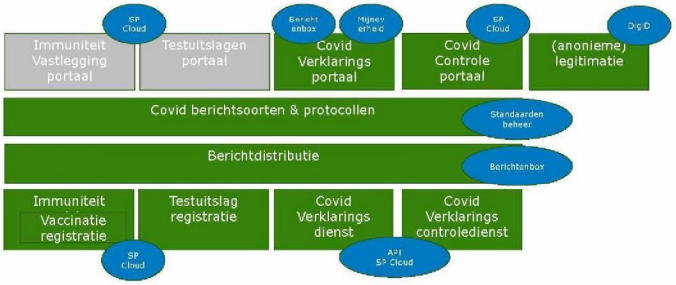
De Nederlandse samenleving heeft al maanden te maken met beperkende maatregelen ter bestrijding van de verspreiding van het SARS-CoV-2 virus. Met de verhoging van de testcapaciteit, de komst van sneltesten, de aanstaande vaccinatieprogramma's en het toenemend aantal burgers dat vrij of immuun is voor Covid, komt de vraag of het mogelijk is om met gebruik van gegevens over het covid-vrij zijn van burgers maatregelen verlicht of opgeheven kunnen worden. De vraag voor deze memo is hoe Logius met haar voorzieningen en/of competenties hier een bijdrage aan kan leveren.

De bestaande voorzieningen van Logius kunnen, gecombineerd met onze de kennis over en rol binnen de GDI, bieden meerdere mogelijkheden om bij te dragen aan een (deel van de) oplossing in een grotere keten om dit vraagstuk op te lossen. Het spreekt voor zich dat er nog onderwerpen omtrent de huidige en toekomstige gegevensverzamelingen rondom testuitslagen en immuniteitsgegevens uitgezocht moeten worden (in samenwerking met VWS/GGD). Tevens moet bekeken worden hoe deze gebruikt mogen en moeten worden om mensen in de fysieke wereld toegang te verlenen.

Vandaar de volgende adviezen met betrekking tot de aanpak:

- Initieer met BZK, VWS en GGD een experteam om te komen tot een snelle oplossing. Start bijvoorbeeld met een pressure cooker van een dag met een aantal "slimme koppen" met een open blik. Betrek hierbij ook user experience en beveiliging/privacy experts.

- Hanteer een bouwblokkenbenadering: Combineer bestaande onderdelen (bv. door API's te gebruiken), en probeert niet om tot een oplossing te komen door één bestaand onderdeel uit te bouwen tot een complete oplossing. Zoek dus niet een complete oplossing in of DigiD, of Berichtenbox, of Bevoegdheidsverklaringsdienst, Mijnoverheid of het SP Cloud platform, maar probeer deze vrijwel ongewijzigd in te zetten voor een totaaloplossing met behulp van bestaande API's. Elke realistische oplossing vereist een samenwerking tussen meerdere partijen. Logius kan op verschillende onderdelen een bijdrage leveren: Zowel op het gebied van technische bouwstenen als ook standaarden, samenwerking en architectuur. Bouwstenen die een rol kunnen spelen in de oplossing staan hieronder schematisch weergegeven. In de groene bouwstenen kan Logius mogelijk een oplossing of significante bijdrage leveren:



Grijs: Component die bij VWS ingericht moet worden.
Groen: Component in het geheel waarbij Logius een bijdrage kan leveren.
Blauw: Product van Logius dat kan bijdragen aan de oplossing.

Op basis van de huidige informatie zien we twee concrete oplossingsrichtingen:

- Gebruik de bouwblokken van Logius samen met een *dedicated* app (bijv. de CoronaMelder) die bijv. een koppeling heeft met DigiD of Mijnoverheid en eventueel ondersteund wordt door het SP Cloud platform. Werk samen met de VWS-ontwikkelaars van de CoronaMelder en de daar gebruikte ontwikkelmethodiek voor de *dedicated app*.

- Gebruik van de Berichtenbox en de Berichtenbox app (in combinatie met DigiD) voor de bezorging en weergave van PDF-documentatie over testresultaat of immuniteit. Daarvoor moet onder andere de impact op het betrouwbaarheidsniveau, de prestatie-eisen (aanleversnelheid) die daarmee samenhangen en de impact die dat heeft op de voorziening Berichtenbox onderzocht worden.

Deze adviezen worden gedaan op basis van de hier verderop uitgewerkte use case met bijbehorende uitgangspunten en aandachtpunten (bijlage 1) en de lijst met mogelijke oplossingen binnen Logius die uit de eerste verkenning gekomen is (bijlage 2).

Voor de volledigheid zijn in bijlage 3 de interne aandachtpunten waar Logius rekening mee moet houden toegevoegd en is er als laatste een lijst met andere mogelijke interessante bouwstenen/initiatieven buiten Logius opgenomen in bijlage 4.

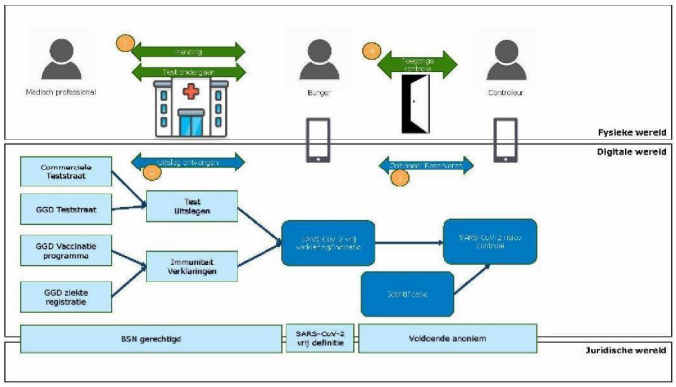
We lichten dit advies graag toe.

Bijlage 1: Beschrijving use case, aandachts- en uitgangspunten

De high-level functionele behoefte is nog niet uitgekristalliseerd. Als vertrekpunt van de analyse is genomen dat een burger aan een commercieel bedrijf wil aantonen dat hij Covid-19 heeft gehad, gevaccineerd is of recent is getest op SARS-CoV-2. Op vertoning van een teken mag hij/zij naar binnen.

Essentieel in deze use-case zijn de volgende elementen: (zie figuur)

- Het inwinnen van de informatie dat iemand SARS-CoV-2 heeft gehad, daarvoor gevaccineerd is of recent een (snel)test heeft gehad.
- Het vaststellen dat deze informatie en/of conclusie betrekking heeft op de persoon die er op dit moment fysiek is
- Het borgen van de zekerheid bij beide partijen dat de informatie betrouwbaar is en alleen voor dit doeleinde gebruikt wordt.



Aandachtspunten:

- Commerciële teststraten hoeven nu alleen positieve testgevallen aan de GGD te melden. Het gaat hier juist om negatieve testgevallen. Dat betekent dat iedere commerciële teststraat een realtime verbinding moet hebben met het uitslagenregister.
- Ook huisartsen en anderen kunnen vaccinaties geven. Het is onbekend of deze informatie met de GGD wordt gedeeld.
- Registratie van ziektegevallen vindt plaats in ziekenhuizen, huisartsen en mogelijk andere plekken. Het is onbekend of dat met de GGD wordt gedeeld.
- Een uitslagen is tijdgeboden. Een negatieve testuitslag heeft maar een beperkte betekenis, omdat daarna iemand alsnog besmet kan worden.

- De Sars-Cv-2 verklaring zal op basis van een aantal bedrijfsregels tot stand komen; is iemand al na de eerste vaccinatie immuun; wordt negatieve uitslag een uur na een positieve uitslag geaccepteerd, etc.
- Enige mate van identificatie is nodig om te weten dat verklaring betrekking heeft op de persoon die aan de deur staat. Maar er hoeft niet bijgehouden te worden wie het is.
- Het gebruik van de mobiele telefoon van een ander. Het kan zijn dat een persoon een mobiel aan een ander geeft met de bijbehorende gegevens. Bijvoorbeeld partners onderling. Of in een vriendengroep. DigiD kan maar op één mobiel actief zijn. De vraag is hoe erg vorm van manipulatie erg is. Een repressieve maatregel zou kunnen zijn om te checken of bijv. deze persoon in de afgelopen vijf minuten als eerder is gebruikt.
- DigiD is primair een authenticatie middel in de digitale wereld en niet voor een fysieke authenticatie/identificatie. DigiD heeft bijvoorbeeld geen beschikking over pasfoto's.
- De controle van een verklaring via bijvoorbeeld DigiD of Mijnoverheid zal vereisen dat er een online verbinding is waarmee de burger het gegeven ter plekke kan tonen en/of de commerciële partij het gegeven ter plekke kan verifiëren. Zodra er op het toegangspunt geen internetverbinding is, werkt dit systeem niet meer. Een ontwerpcriterium kan zijn dat het offline gebruikt moet kunnen worden.
- Er kan een groep personen zijn die niet deze middelen wil gebruiken en de voorkeur geeft aan een niet-digitaal, fysiek proces.
- Het introduceren van deze systematiek kan ervoor zorgen dat er een run op tests komt. Het is denkbaar dat er teststraten worden ingericht naast uitgaansgelegenheden. In dat geval zal dat een hoge druk geven op volume, beschikbaarheid en tijdigheid van de gegevensuitwisseling. Tevens zijn piekmomenten voor, rond en in het weekend te verwachten.

Uitgangspunten voor een oplossing:

- Continuïteit: Bestaande (vitale) infrastructuurdiensten mogen door de oplossing niet in gevaar komen, zowel technisch als qua maatschappelijke acceptatie niet.
- Vertrouwen: de oplossing moet maatschappelijk geaccepteerd zijn.
- Verantwoordelijkheden: de rollen en verantwoordelijkheden moeten helder worden vastgesteld.
    - De medisch professional moet de gegevens tijdig en waarheidsgetrouw vastleggen en uitwisselen.
    - De burger bepaalt wie welke gegevens mag zien. Het mag niet zo zijn dat een controleur een directe bevraging bij een bron doet, zonder dat dat in opdracht van de burger is.
    - De controleur bepaalt of iemand toegang krijgt. Het systeem heeft een ondersteunende functie. Het is niet de bedoeling dat het systeem de controlerende rol volledige uitvoert. Een oplossing waarbij een poortje alleen opengaat als de juist gegevens worden ingevoerd is dus uitgesloten. Analoog aan een douanecontrole.
    - De rol van de overheid in het samenstel is duidelijk: Faciliteert het proces tussen bovenstaande rollen en verantwoordelijkheden. De overheid is niet de alles bepalende beslisser.

- Privacy: persoonsgerelateerde en medische informatie wordt niet onnodig opgeslagen bij commerciële en publieke organisaties en alleen die informatie die nodig is voor het vaststellen van een veilige conclusie wordt gedeeld.
- Haalbaarheid: tijd gaat boven geld. De oplossing moet voldoende snel te realiseren zijn om van nut en betekenis te zijn.
- Gebruiksvriendelijkheid: het is makkelijk te begrijpen en bestaat uit enkele simpele stappen voor beide partijen.
- Beschikbaarheid: De oplossing moet een voldoende hoge (24x7? of 18x7?) beschikbaarheid hebben.
- Performance: De performance moet voldoende zijn om in een paar seconden te kunnen vaststellen of iemand toegang heeft.
- Voldoen aan wet- en regelgeving. Eerst wordt een oplossing binnen bestaande wet- en regelgeving gezocht. Als bovenstaande principes in een andere oplossingsrichting zoeken, kunnen eventuele uitzondering/wijzigingen op wet- en regelgeving worden voorgesteld.
- Integriteit: de controle is niet op eenvoudige wijze te manipuleren. En er bestaat de kans dat manipulatie in ieder geval steekproefsgewijs gedetecteerd wordt.
- Techniek: Het moet zo simpel mogelijk zijn en hergebruik van bestaande zaken heeft een voorkeur, omdat de doorlooptijd beperkt is.

Bijlage 2: Verkende oplossingen binnen Logius

Een eerste verkenning rondom bestaande Logius bouwstenen en ontwikkelingen die een mogelijke invulling geven aan de use case van bijlage 1 levert de volgende (theoretische) mogelijkheden op:

1. **Het tonen van het gegeven in de Berichtenbox App**. Gebruiker logt ter plekke in op de berichtenbox app (via app2app DigiD) en toont een relevant bewijs dat als brief naar de berichtenbox gestuurd is. Aandachtspunt: Aan de deur is deze optie mogelijk omslachtig en er zitten veel meer privacy gevoelige brieven in de app. Daarnaast is de verwerkingstijd van brieven in Globe nu max 24 uur (SLA tijd).

2. **Het opnemen van een groene vink als tabblad in DigiD.** De burger logt ter plekke in; de gegevens worden opgehaald en resulteren in een groen scherm. Controleur accepteert dat en gebruikt dat om te bepalen of iemand toegelaten is. Aandachtspunt: Mensen kunnen screenshot gebruiken; telefoon van een ander gebruiken; geldigheid moet in beeld staan.

3. **Het tonen van het gegeven in de Mijn Gegevens App.** Deze app en de achterliggende infrastructuur is nog in ontwikkeling. Versnelling om dit in minder dan drie maanden gerealiseerd te krijgen met voldoende kwaliteit lijkt onrealistisch. Uitvoering van app ontwikkeling gebeurt nu via inbesteding bij de Belastingdienst.

4. **Het tonen van het gegeven in MijnOverheid**. Gebruiker logt ter plekke in met DigiD op Mijnoverheid, waar op een GGD dashboard de SARS-Cov-2 status getoond wordt. Aandachtspunt: Aan de deur is ook deze optie omslachtig.

5. **Het scannen van een QR code bij het bedrijf**, waarna de DigiD app doorschakelt naar het RIVM en daar aangeeft dat de persoon vrij is van Covid. Aandachtspunt: Aan de deur zijn de stappen van een website bezoeken en DigiD gebruiken best veel voor een vlotte toelating.

6. **FBS Notificatie service / MijnOverheid notificatie service**. Gebruik de notificatie services (en profielen) om notificaties te versturen waar een link naar een bewijs (bv. Tijdsgebonden QR code) is te vinden. Aandachtspunt: Nu is het juist de policy vanuit phishing om geen links in de emails te hebben.

7. **Het ontwikkelen van een specifieke app voor dit doel.** Na opstarten van de app logt je via DigiD één keer in bij RIVM en geef je toestemming de gegevens via de app uit te wisselen (voor langere tijd). De gebruiker opent de app aan de deur, waarna de status opgehaald en getoond wordt. Aandachtspunt: Telefoon van een ander wordt gebruikt/uitgeleend.

8. **Het inpassen van de functionaliteit in de CoronaMelder app.**
   Voordeel: de hele app-infrastructuur en GGD koppeling is daarvoor al beproefd. Logius helpt met DigiD/MO koppelingen.

9. **Het ontwikkelen van architectuur en/of protocollen voor gegevensuitwisseling van een digitaal vaccinatie/covidvrij paspoort.**
   Logius kan architectuur en stelsel/standaardbeheer diensten bieden om een bijdrage te leveren.

10. **Het bieden van een SP-Cloud platform voor de hosting.**
    Aandachtspunt: 24x7 (of 18x7) moet wel geregeld zijn.

Bijlage 3: Aandachtspunten voor Logius

Bij de nadere uitwerking van de oplossingsrichtingen levert de verkenning de volgende aandachtspunten op voor Logius:

Organisatorisch

- Het is niet helder wie de opdrachtgever is, welke use-cases wel of niet aanvaardbaar zijn en welke randvoorwaarden gelden. Daardoor is het moeilijk concrete uitspraken te doen over de wenselijkheid en (technische) haalbaarheid. Voor een succesvol ontwikkeltraject moet opdrachtgeverschap en afspraak wie de requirements opstelt helder worden.
- Elementen als de juridische aspecten, vereiste wet- en regelgeving, impact op de samenleving, etc. zijn buiten scope geplaatst. Deze kunnen echter wel de randvoorwaarden van de oplossingen beperken waardoor sommige afvallen, of andere juist in beeld komen. Het totstandkomen van de uiteindelijke oplossing zal multi disciplinair afgestemd moeten worden.
- *Capaciteit en competenties* (nog). De app ontwikkeling van Logius is momenteel inbesteed bij de Belastingdienst. Als dit met een nieuwe app gerealiseerd gaat worden, is de opschaling daarvan een uitdaging die interdepartementale afstemming vergt. Tevens kan de vraag komen of dit niet met een aanbesteding gerealiseerd moet worden.
- Het tonen van de gegevens is maar een klein onderdeel van de totale propositie. Belangrijkste vraagstuk is hoe de infrastructuur opgezet kan worden om betrouwbaar, efficiënt en met inachtneming van de privacy de set van gegevens uitgewisseld kan worden tussen de partijen. Voor een succesvolle implementatie zal ook dit aspect goed uitgewerkt moet worden. Bovendien is coördinatie over het totaal noodzakelijk om het te laten functioneren.
- Het is niet duidelijk hoe lang het gaat duren voor de eerste oplossing er kan zijn en hoe lang het zinvol is om een oplossing te hebben. Het inregelen van een nieuwe app met bijbehorende infrastructuur zal – afhankelijk van de mate van hergebruik – een doorlooptijd van 3-9 maanden hebben als er een aanzienlijke capaciteit op wordt ingezet. Dat moet worden afgewogen tegen de restkans en ernst van Covid in relatie tot een reeds gedeeltelijk gevaccineerde populatie en bestaande medicatie. Ook daar kan het zijn dat op een termijn van 3-9 maanden een aanzienlijk deel van de populatie is gevaccineerd, danwel dat er door betere behandelmethoden de ernst van Covid in relatie tot andere ziektebeelden is gezakt.

Impact huidige voorzieningen

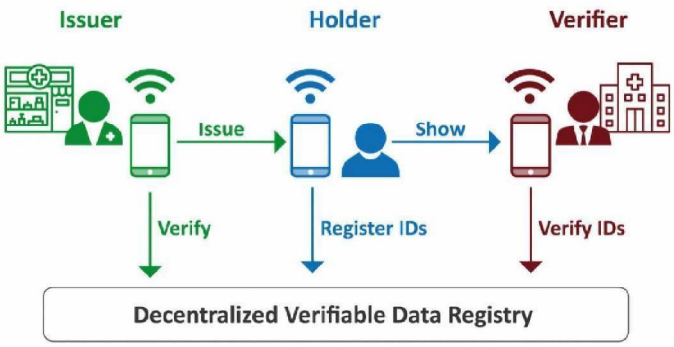
- *Functievermenging/imago DigiD, MijnOverheid,...* Het Covid-vrij aspect is in principe van tijdelijke aard. Bij inpassing in DigiD / Mijnoverheid wordt het gebruik van de app associatief verbonden met het virus, waardoor het imago mogelijk geschaad wordt. Zo kan bijvoorbeeld (onterecht) de indruk ontstaan dat de BSN gegevens worden gedeeld met commerciële partijen. Of dat bij iedere toegang tot een uitvoeringsinstantie

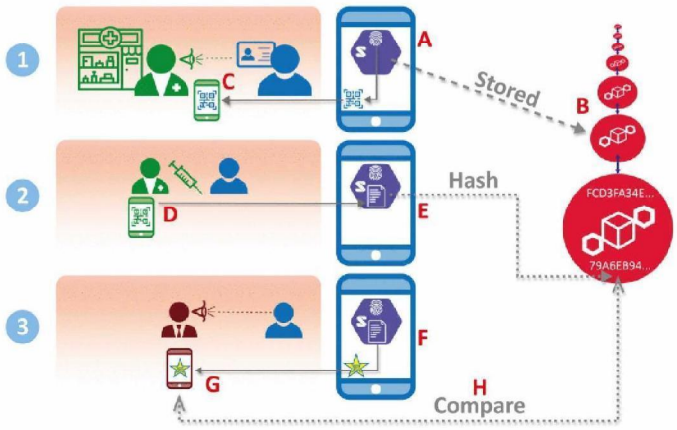
automatisch ook de medische gegevens meekomen. Of dat "bij de overheid alle data intern gedeeld wordt".

- *Functieverbreding naar digitaal paspoort*. Door het opnemen van dergelijke gegevens kan de indruk onstaan dat een eerste stap gezet in verbreding van DigiD als toegangsmiddel naar DigiD als een digitaal paspoort. DigiD gaat dan namelijk in de fysieke wereld gebruikt worden als identificatiemiddel. Er moet immers een link gelegd worden tussen de persoon die ergens naar binnen wil en het bewijsstuk dat aangeeft dat er geen actieve besmetting kan zijn.
- *Functieverbreding naar medisch dossier*. Een tweede functieverbreding is dat er medische gegevens aan het toegangsmiddel worden gekoppeld. Naast het element "vrij van x" kan doorgegroeid worden naar "gevaccineerd tegen x" of zelfs "lijdend aan ziekte x" en "gebruiker van medicijn x". Het zetten van de eerste stap opent de discussie of deze toepassingen wel of niet zinvol zijn en kan doorlooptijd verlengen en succes van implementatie beperken.
- *Medische gegevens*. Het immuun zijn voor Corona (door vaccinatie of reeds doorlopen ziekte) c.q. het recent negatief getest zijn op kan gezien worden als een medisch gegeven. De verwerking van medische gegevens stelt in potentie extra eisen aan functionaliteit en beheer van bestaande voorzieningen en gegevensuitwisseling.
- *BSN gerechtigd zijn*. Het gebruik van DigiD is omvat ook het verwerken van BSN gegevens. Bij de use-case om controleurs van commerciële bedrijven te laten controleren op "vrij-van-corona" moeten maatregelen genomen worden dat dit kan zonder de verwerking van BSN gegevens. Tevens moet communicatief duidelijk gemaakt worden dat dat niet gebeurt. Het wetgevingskader en overeenkomsten moeten (mogelijk) aangepast worden om het gebruik bij commerciële ondernemingen toe te staan.
- *Betrouwbaarheid*. Het tonen van een vinkje op een groen scherm geeft geen hoge betrouwbaarheid. Het is vrij makkelijk om en screenshot van een ander te gebruiken of zelf een fake screenshot te maken. Het bouwen van methoden om de verificatie uit te voeren is compleet nieuw.

Bijlage 4: Andere initiatieven en interoperabiliteit

- De CoronaMelder app is na een *hackaton* op een open manier ontwikkeld, waarbij privacy en veiligheid een nadrukkelijke rol hebben gespeeld. Hiermee is een standaard en verwachting gezet voor aanvullende functionaliteit en soortgelijke ontwikkelingen. Daarom is het handig om eerst af te wegen of dit niet (1) een onderdeel van de CoronaMelder of een zusterapplicatie moet worden en (2) met hetzelfde ontwikkelteam en (3) met dezelfde werkwijze ontwikkeld moet worden.
- Via IRMA is ervaring opgedaan met Digitale Wallets. Je zou samen met IRMA kunnen onderzoeken of de systematiek (her)gebruikt kan worden voor deze use case.
- Common Ground (van VNG realisatie) heeft NLX (https://nlx.io) ontwikkeld, een open bouwsteen voor het privacy vriendelijke uitwisselen van informatie. Deze is mogelijk bruikbaar in de totaaloplossing. Dit is compatible met SP Cloud.
- De IATA werkt aan een *travel pass* met soortgelijke doelstelling, maar dan in internationaal verband https://www.embs.org/ojemb/articles/covid-19-antibody-test-vaccination-certification-theres-an-app-for-that/. Als iedere sector met een eigen oplossing komt kan dat verwarring geven. Het kan een strategie zijn om juist in te zetten op bijdragen aan bestaande internationale alternatieven.
- Voor de Engelse NHS is een architectuur ontwikkeld en er wordt nu gewerkt aan de bijbehorende infrastructuur en apps. https://ieeexplore.ieee.org/document/9105054.





- Het patroon lijkt op de vraagstukken rondom de leeftijdscontrole in supermarkten en de Woco pilot. Daar is echter het vraagstuk op te lossen met het ophalen van een gegeven uit het stelsel van basisregisters, terwijl het hier om extra gegevens gaat. Voor de nieuwe typen meldingen is nog geen register vastgesteld.